

Nebraska Attorney General's Office

Consumer Protection Division 2115 State Capitol Building Lincoln, NE 68509

(402) 471-2682

Protect The Good Life. Nebraska. gov

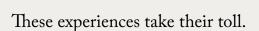


Dear Fellow Nebraskans,

We enjoy a wonderful state with strong roots and hard-working citizens who are surrounded by plentiful resources. One of our greatest gifts is the neighbor we know next door.

We wish that everyone were truly "Nebraska Nice" and treated their neighbors with the respect they deserve; however, sadly, scam artists from across the country and around the world attempt to defraud Nebraskans every day. This is especially true within our state's senior population.

This fact is well-documented by fraud reports. We know seniors are exploited. Seniors tell us their stories of annoyance, frustration, and pressure exerted by scammers.



Elder fraud and abuse are more than a frustration and nuisance; they are a real threat and one that is impacting not only quality of life but the length of life as well. For the sake of our families, we must push back.

Education is the best weapon we have in preparing people to protect themselves. This guide includes information on how to spot, stop, and avoid potential loss if you or someone you know is a target of fraud.

Should you experience uncertainty, have feelings of fear or concern, or just wish to pose a question, please call our Consumer Protection Division and let us be of service. We are here to protect and help you.

In the meantime, trust your instincts. If something seems too good to be true, it probably is.

Sincerely,

Douglas J. Peterson Nebraska Attorney General





Table of Contents

	Imposter Scams)
	Identity Theft1	0
	Foreign Lottery1	3
	Charity Fraud1	5
7	Home Repair Scams1	8
\$	Investment Fraud	21
	Bogus Business & Job Opportunities2	23
	Reduce Junk Mail & Unwanted Telemarketing Calls2	26
	Top Consumer Tips3	1
	Important Phone Numbers	33
(3)	Important Websites & Email Addresses3	34



Scammers may create fake personas to get you to believe that their story is legitimate.

Some pose as friends or relatives stranded in foreign countries without money; others claim to be working for or affiliated with a government agency.

If you suspect a scam, hang up.

Look for the warning signs that may indicate a scam:

- You receive a call or email alleging you've won a prize or that something is terribly wrong - taxes are unpaid, your government benefits will be lost, a family member is in trouble, or your computer has been compromised.
- The caller asks you to send them money immediately preferably by wire transfer or gift card. Credit cards or checks are discouraged.
- The caller may ask for access to your computer or other confidential information such as your Social Security number, date of birth, bank account, or credit card numbers.
- The caller is insistent and offers to call you back or stays on the line while you do what they are asking you to do.

Types of Imposter Scams:

Romance Scam: This type of scam often entails an entire online persona carefully crafted, frequently using pictures stolen from social media sites to be the ideal person. These relationships can go on for quite some time before the signs start appearing, but they invariably lead to requests for money.

Grandparent/Family Emergency

Scam: A grandparent receives a phone call (or sometimes an e-mail) from a "grandchild." Usually, the person claims to be traveling, in trouble, and needs money wired.

Fake Debt Collector: These scammers pretend to be a debt collection agency collecting on a loan you took out years ago. Sometimes they create a fictional loan; sometimes, they use a real loan that was either paid off or discharged. Either way, they will be aggressive and persistent.

Government Imposter Scams:

You get a call or an official-

looking
letter. The
imposter
claims to
be from, or
affiliated
with, a
government
agency
such as



Administration, or Medicare. They threaten to arrest you, take away your benefits, or take you to court if you don't pay the debt you supposedly owe. They may also trick you into providing confidential information.

Computer Technical Support:

You receive a call from someone claiming to be a computer tech associated with a well-known company like Microsoft. They say they've detected viruses or other malware on your computer and trick you into giving them remote access or paying for software or a "fix" you don't need.

What you should do if you suspect a scam:

- Resist all pressure to make a decision immediately.
- Hang up. The longer a scam artist is allowed to talk, the more likely it is you will be persuaded.
- Unless you initiate the phone call or have a prior relationship with the caller, NEVER give

Don't respond to calls requesting your personal information.

personal
information
over the
phone, even
if the caller
asks you to
"confirm"
this
information.
It's a trick.

- Get all information in writing before you agree to buy.
- Don't pay for something just because you'll get a "free gift."
 Don't agree to any offer for

which you have to pay an administration, registration, or shipping fee to get a prize or gift.



• Don't send cash by messenger, overnight mail, wire transfer, gift card, or prepaid card. If you use cash or a money transfer — rather than a credit card — you may lose your right to dispute fraudulent charges. The money will be gone.



Identity theft often tops the list of consumer complaints reported nationally.

Cases involving government documents and benefits — including Medicare, Medicaid, and tax returns — are rising fastest, followed by new account origination (bank accounts and credit cards), and utility bills, including those for cable TV and cell phones.

Look for the warning signs of identity theft:

- You are denied credit.
- You get a notice from the IRS about a tax debt that you do not believe is yours.
- You find charges on your credit card or withdrawals from your account that you don't remember making.
- Personal information, credit cards, ATM cards, checks, or IDs have been stolen from you.
- You suspect someone has fraudulently changed your mailing address.

How they hook you:

• Phishing. Phishing is a form of misrepresentation designed to dupe you into revealing your confidential information. It comes in a variety of forms, often appearing as messages from businesses you trust.

- Mail Theft. Identity thieves are prone to stealing mail, looking specifically for pre-approved credit card and insurance offers.
- Family, Friend, or In-home Employee. More than half the time, the thief is a family member, friend, neighbor, inhome employee, or someone at a business you frequent.
- Skimming Devices. Skimming is when the information on a credit card is copied then loaded onto a fake card to be used fraudulently. It most frequently occurs in restaurants and at the gas pump.

Never give personal information over the phone.

What you should do to prevent identity theft:

- Don't carry your Social Security or Medicare card in your wallet.
- Be wary of requests by phone for your personal information. Don't respond to incoming phone calls from strangers requesting your personal information. Be especially wary of calls from alleged government agencies.
- Secure your information. Keep all of your sensitive personal documents, including financial documents, in a safe, secure, locked place.
- Shred it. Shred personal and financial records with a microcut shredder before throwing them away.
- Protect your computer. Consult with a computer professional to make sure your computer system is secure. Install antivirus software, anti-spyware, and

firewall software to guard against hackers that steal personal information.

- Check your credit regularly.
 Request a free credit report
 at www.annualcreditreport.
 com on a regular basis. You can
 request one free credit report
 per year from each of the three
 major credit reporting agencies,
 thereby allowing you to check
 your credit three times per year
 for free.
- Consider placing a freeze on your credit report. This free tool lets you restrict access to your credit report which makes it more difficult for identity thieves to open new accounts in your name.





Be careful! Most promotions for foreign lotteries are likely to be phony.

Lottery scammers may pressure you to send money immediately via wire transfer or prepaid card. They may even use your bank account numbers to make unauthorized withdrawals or credit card numbers to run up additional charges.

Look for the warning signs that may indicate a scam:

- Phantom Riches: News of an offer sounding too good to be true, but one with strings attached.
- **Urgency:** You are pressured to make an immediate decision, take immediate action.
- Payment via Money Transfer: Upfront payment by money transfer is required prior to receiving your free prize, gift card, prepaid card, or other payment.

If you respond to a foreign lottery letter or call, you may be placed on a "sucker list."

• Probes for Personal Identifying Information: You are asked to reveal personal information such as Social



Security number, date of birth, bank account information, etc.

What you can do to protect yourself:

- Ignore all mail and phone solicitations for foreign lottery promotions. You cannot win a contest you did not enter.
- Screen your calls using Caller ID and related services like Anonymous Call Rejection and Selective Call Rejection.
- Don't give out your credit card and bank account numbers and never wire money to someone you haven't met.
- Just hang up the phone. It's okay to be rude!



Charity fraud occurs when an individual or group deliberately misrepresents its fundraising intentions or solicits funds for phony causes.

Fraudulent fundraisers use many of the same techniques as reputable fundraisers, but they may do so in a questionable or illegal

way.

Look for the warning signs that may indicate a scam:

• The charity refuses to give you

Don't respond to calls requesting wire transfers.

full details about the group's identity, mission, costs, and how it will use your donation.

- The charity cannot, or will not, send you a brochure or donor form, or does not have a website you can visit. If they do have a website, it may appear hastily constructed.
- You are asked to give or send cash or transfer money by wire or prepaid card. The caller refuses to let you send a check.

How they hook you:

The following fundraising techniques are questionable and, in some cases, illegal:

- Sound-alike names: Fraudulent charities take names very similar to those of high-profile charities known and trusted by the public.
- High-pressure tactics:
 A solicitor urges you to
 give money (usually cash)

give money (usually cash) immediately and before you even have a chance to review the information.

• Deceptive bills and invoices:
These claim that an amount is owed or promised to a charity when no such commitment was made.



- Prize offers: You are told you have won a contest and are eligible for a prize if you donate to a charity.
- Unsolicited Gifts: Usually just tokens, these "gifts" are enclosed in direct mail solicitations to make you feel obligated to give something back.

What you should do if you suspect a scam:

- Log on to www.give.org, the website of the Better Business Bureau's Wise Giving Alliance, or visit the websites of charity watchdog evaluators www. charitynavigator.org or www. guidestar.org.
 - Ask for a brochure or other written materials to be sent to you in the mail.
 - Ask for the name, address, and phone number of the charity and a copy of the charity's tax-exempt letter indicating its IRS status. You can't claim a tax-deductible

donation if the charity does not have one.

- Ask how your money will be used and what percentage of your donation goes directly to the cause. Legitimate charities will have ready answers because they are used to the question.
- Never give cash. Make your contribution in the form of a check payable to the full name of the charity.
- Don't give out your Social Security number. A charity does not need it in order for you to claim a tax deduction.





If someone who claims to be a repair expert or contractor knocks on your door and offers you a "deal," be skeptical.

You could end up the victim of work started but never completed or shoddy workmanship for a job that did not need to be done at all.

Look for the warning signs that may indicate a scam:

- An unsolicited "contractor" knocks on your door saying they were working in the neighborhood and have "extra material" they didn't use for which they will offer you a special deal available that day only.
- The "contractor" is unable to show proper identification, such as a permit allowing them to do the type of specialized home repair, and refuses to provide an estimate or references.
- You are pressured to make a decision immediately.
- A demand for up-front payment is made for services either not yet performed or incomplete.
- A small repair suddenly becomes a big problem.

What you should do if you suspect a scam:

- Refuse to purchase services from any contractor who shows up uninvited at your house.
- Never agree to have work done on the spot. Determine what you want done and seek qualified contractors.
- Use a local, well-established contractor. Ask for references and check with other customers to find out if they were satisfied with the work performed.



• Shop around for a good price. If you are having major work done, get several competitive bids in

writing. Be wary of any bid that seems too good to be true.

• Do not pay the full amount upfront or other unreasonable

advance sums. Negotiate a payment schedule tied to the completion of the job and pay by check or credit card. Do not pay with cash.

- If a contractor pressures you to buy his services, look elsewhere for your home repair needs.
- Check for qualifications like registration and licensing. The Nebraska Contractor Registration Act requires contractors and subcontractors doing business in the state to register with the Nebraska Department of Labor. You can search all currently registered contractors and subcontractors on the Nebraska Department of Labor's website at www.dol. nebraska.gov or by calling (402) 471-2239.
- Cities may also require certain professionals, such as electricians and plumbers, to hold specific licenses. Contact your city government before agreeing to anything.



Seniors lose millions each year in "get rich" schemes that promise high returns with low or no risk.

Many of these scams are perpetrated by people posing as licensed investment professionals, estate planners, prepaid funeral consultants, or salespeople with an "incredible business opportunity." Look for the warning signs that may indicate a scam:

- The person will not take time to answer questions and instead urges you to leave your money in their hands.
- High-pressure sales tactics to rush you into a decision and send money immediately (by overnight courier or money transfer) to secure your stake in their "sure-fire" investment.

- Vague information about the nature of the investment focusing instead on the money you'll make.
- Requests for your bank account, Social Security, or other private account numbers. This information is rarely, if ever, needed and should never be given to someone you don't know or trust.

What you should do if you suspect a scam:

• Take your time. When making a decision about investments, consult with someone you can

Don't buy anything you don't understand. trust to collaborate on your investment decisions.

• Do some research. It's best to get an independent appraisal of the specific asset, business, or investment you're considering.

- Be skeptical. Be particularly suspicious of sales pitches that play down risk or portray written risk disclosures as routine formalities required by the government.
- Find out who you're dealing with. Do an internet search with the name of the company and words like review, scam, or complaint.
- Get the track record of the company you're considering investing in and the background of the people promoting it. Ask for written proof of how much of your money is going to the actual investment and how much is going to commissions, promoters' profits, and marketing costs.





Scammers push empty promises of wealth from ideas so detailed and timely that the deal just has to be legit... at least, that's what they want you to think!

Take the time to ask the questions that can keep you from getting ripped off.

Look for the warning signs that may indicate a scam:

• A company or person claims they can offer you a "guaranteed" job placement or a "risk-free" business opportunity.

- You are required to pay an upfront fee for a business plan or other materials associated with an opportunity.
- The job only requires you to transfer money for someone else.
- Promises of guaranteed income or substantial returns with little work.

How they hook you:

Medical Billing: You are charged a fee of hundreds, even thousands of dollars, to be provided everything you need to launch your business.

Legitimate companies don't charge people to work for them.

Few consumers who pay for medical billing

opportunities ever find clients or make any money.

Envelope Stuffing: Promoters advertise that for a "small" fee,



they'll tell you how to earn big money stuffing envelopes at home. Promises of big earnings through envelope-stuffing are false.

Assembly or Craft Work: Ads state you can make money assembling crafts or other products at home. You invest hundreds of dollars for equipment or supplies or spend hours producing goods for a company that has promised to buy them only to find the company doesn't pay you — supposedly because your work isn't "up to standard."

Rebate Processing: An ad or email says you can earn big money by helping to process rebates.

The fee for training, certification, or registration is nothing compared to what you'll supposedly earn processing rebates from home. There are no rebates to process, and few people ever see a refund.

Government Job Scams: Ads in newspaper classified sections or online offer — for a fee — to help you find and apply for federal jobs. You're charged a fee for your application and study materials — for a job that never materializes.

Mystery Shopper Scams:

Newspaper ads and emails create the impression that mystery shopping jobs are a gateway to a high-paying job with reputable companies. You first must register and pay a fee. The registration and certification are almost always worthless. Often, your first job is to evaluate the effectiveness of a money transfer service. You will unknowingly be given a fake check, told to deposit it in your bank account, withdraw the same amount in cash and send it by wire transfer to a third party. The

check will bounce, and you will be out the cash.

What you should do if you suspect a scam:

- Do your research before you commit to any money-making opportunity. By law, business opportunity promoters must give you certain information before you hand over any money.
- Remember: legitimate companies don't charge people to work for them; they pay people to work for them.
- Avoid opportunities that require you to deposit checks into your personal bank account, withdraw the amount

in cash, and wire it to a third party. The check is a fake.







Americans receive nearly 80 billion pieces of advertising mail every year.

If you want to reduce unwanted mail or telemarketing calls, you can do something about it.

Reducing Junk Mail

You can eliminate your junk mail. The Data & Marketing Association lets you opt-out of receiving unsolicited commercial mail from many national companies for ten years by registering your preferences through their consumer website www.DMAchoice.org. When you register, your name will be put on a "delete" file and made available to direct-mail marketers and organizations. This will reduce most of your unsolicited mail. However, your registration will not stop mailings from organizations that do not use DMAchoice.

To register your preferences with the DMA, go to www.DMAchoice.org (there is a \$2 processing fee), or mail your request with a \$3 processing fee to:

DMAchoice
Data & Marketing Association
P.O. Box 900
Cos Cob, CT 06807



Email

The DMA also has an Email Preference Service to help you reduce unsolicited

commercial emails. To opt-out of receiving unsolicited commercial email from DMA members, visit www.DMAchoice.org.
Registration is free and good for six years.

Telemarketing

The federal government's National Do Not Call Registry is a free, easy way to reduce the vast majority of telemarketing calls you get at home. The exceptions are political calls, charitable calls, and marketing research/survey calls, and calls from businesses with whom you already have a relationship.

To register your phone number

or to get information about the registry, visit www.donotcall. gov, or call 1-888-382-1222 from the phone number you want to register. The registry works for both landlines and cell phones. You will get fewer telemarketing calls within 31 days of registering your number.

Provided you do not move or obtain a different telephone number, you do not need to register more than once. The registry does not expire. Telephone numbers on the registry will only be removed when they are disconnected and reassigned, or when you choose to remove a number from the registry.



Unwanted Calls

Stopping Unwanted Calls on Your Landline. Ask your local phone company about custom calling features. These features can be easily activated and deactivated on your phone through quick-dial combinations known as star codes. Popular and often free calling features include Anonymous Call Rejection (*77), Selective Call Rejection (*60), and Selective Call Acceptance (*64).

Stopping Unwanted Calls on Your Mobile Phone. Stopping unwanted calls on a mobile phone is dependent on your phone's operating system and carrier. Three main avenues of defense include:

• Built-in Features – Recent mobile phones offer a native call-blocking feature. Tutorials to assist can be found by searching video-sharing websites online.

• Carrier-provided Features –

Wireless network carriers offer services effective at identifying

and blocking unwanted calls. Some services are free; others carry a nominal

Ask your local phone company about custom calling features.

fee. Check with your carrier to learn more.

• Call-blocking Apps – Thirdparty apps are available to block unwanted calls. Some apps may require access to your contacts or call history information. Make sure you have read and understood the app's Terms of Service and Privacy Policy prior to installation.

Unwanted Credit and Insurance Offers

If you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt-out of receiving them for five years or opt-out permanently.

To Opt-Out for Five Years:

Call toll-free 1-888-5-OPT-OUT(1-888-567-8688), or visit www.optoutprescreen.com. The phone number and website are operated by the consumer reporting companies.

To Opt-Out Permanently:

You may begin the permanent Opt-Out process online at www.optoutprescreen.com. To complete your request, you must return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

When you call or visit the

website, you'll be asked to provide certain personal information, including your name, Social Security number, date of birth, and home telephone number. The information you provide is confidential and will be used only to process your request to opt-out.

If you do not have access to the Internet, you may send a written request to permanently opt-out to each of the major consumer reporting companies (i.e., Equifax, Experian, and TransUnion). Make sure your request includes your name, Social Security number, date of birth, and home telephone number. For your protection, it is recommended the request be sent Registered Mail or Certified Mail.





- If it sounds too good to be true, it probably is.
- Everyone, regardless of age, sex, education level, financial situation, or where they live, is a potential victim — including seniors.
- Seniors may be targeted more because they are perceived by scam artists to have more free time, a willingness to talk, or

may be more trusting.

- Be direct, rude if you have to be. Don't be afraid to hang up the phone or shut the door on unwanted solicitations.
- Concede frustration and embarrassment, but do not feel ashamed should you fall victim to a scam artist's tactics. They are professionals skilled in the art of persuasion.

- Never pay money upfront to collect a prize. Free is free.
- Be aware that wiring money is just like sending cash. Once you send it, it is gone for good. The same applies to sending money using prepaid cards.
- Do not buy what you do not understand.
- Ask a neighbor, family member, friend, banker, or trusted advisor if you have doubts about an offer or business.
- Caller ID can help you guard against annoying phone calls and potential scam artists.
 Remember: "If Caller Unknown, leave it alone!"
- Strengthen Caller ID with the addition of at least two calling features: Anonymous Call Rejection and Selective Call Rejection. Virtually all telephone carriers offer these services for a nominal additional fee, if any.
- Review financial statements

- regularly.
- Order your free credit report once a year through www. annualcreditreport.com.
- Shred personal and financial records with a micro-cut shredder before throwing them away.
- Call law enforcement immediately if you think you have been victimized.
- Never accept the help of someone who calls and offers to help you recover the losses in a scam "for a small fee." Odds are it is the same scam artist coming back for more.



Important Phone Numbers

Nebraska Attorney General's Office	402-471-2682
Nebraska Attorney General's Consumer Division	800-727-6432
Nebraska Association of Area Agencies on Aging	402-441-7070
State Health Insurance Information Program (SHIIP)	800-234-7119
Senior Medicare Patrol (SMP) (Medicare & Medicaid Fraud Waste)	877-808-2468
Adult Protective Services	800-652-1999
Better Business Bureau	800-649-6814
Contractor Registration Certificates	402-471-2239
National Do Not Call Registry	888-382-1222
Federal Trade Commission	877-382-4357
Federal Communications Commission	888-225-5322
U.S. Postal Inspection Service	877-876-2455
Free Credit Report	877-322-8228
Opt-Out (protect your credit by opting out of prescreened credit and insurance offers)	888-567-8688



Nebraska Attorney General's Email ago.consumer@nebraska.gov Nebraska Attorney General's Main Website ago.nebraska.gov Nebraska Attorney General's ProtectTheGoodLife.Nebraska.gov Consumer Website Nebraska Association of Area Agencies www.nebaaaa.org on Aging National Do Not Call Registry www.donotcall.gov Better Business Bureau's Charity Registry www.give.org Charity Navigator www.charitynavigator.org (America's largest independent charity evaluator) Federal Trade Commission www.ftc.gov Free Annual Credit Report www.annualcreditreport.com Contractor Registration Verification www.dol.nebraska.gov Mail and Email Preference Service www.DMAchoice.org Opt-Out www.optoutprescreen.com (protect your credit by opting out of prescreened credit and insurance offers)

